Maximally entangled states in pseudo-telepathy games

Laura Mančinska[1]

Centre for Quantum Technologies, National University of Singapore

Abstract. A pseudo-telepathy game is a nonlocal game which can be won with probability one using some finite-dimensional quantum strategy but not using a classical one. Our central question is whether there exist two-party pseudo-telepathy games which cannot be won with probability one using a maximally entangled state. Towards answering this question, we develop conditions under which maximally entangled states suffice. In particular, we show that maximally entangled states suffice for weak projection games which we introduce as a relaxation of projection games. Our results also imply that any pseudo-telepathy weak projection game yields a device-independent certification of a maximally entangled state. In particular, by establishing connections to the setting of communication complexity, we exhibit a class of games G_n for testing maximally entangled states of local dimension $\Omega(n)$. We leave the robustness of these self-tests as an open question.

Keywords: nonlocal game, entanglement, projection game, maximally entangled state, pseudo-telepathy, self-testing

1 Introduction

Entanglement is a central feature of quantum information processing (see [Gru99] or [NC10] for a general introduction). In many cases it can be used to perform nonlocal tasks that would otherwise be impossible or very inefficient. Therefore, entanglement is a resource and one is interested in means of measuring the entanglement content of a quantum state. Many such entanglement measures have been introduced and studied (see [PV07] for a survey). The usual approach is to define entanglement as the resource that cannot be increased using local quantum operations and classical communication (LOCC). Here, we will only be concerned with the two-party scenarios. In such a case, any desired shared state can be obtained via LOCC from the so-called *maximally entangled state*

$$|\Psi_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle.$$

Therefore, according to any entanglement measure, the state $|\Psi_d\rangle$ possesses the highest entanglement content among all states in $\mathbb{C}^d \otimes \mathbb{C}^d$. It would perhaps be natural to expect that maximally entangled states are the most useful ones

for accomplishing nonlocal tasks. It turns out that this intuition fails and there are known examples where less entangled states allow for better performance [ADGL02,AGG05,ZG08]. Moreover, in some cases, maximally entangled states are shown to be suboptimal even if we do not restrict the dimension d of the maximally entangled states [JP11,VW11,LVB11,Reg12]. Most of these examples are given in terms of Bell inequality violations and when stated in terms of nonlocal games they yield games at which entangled players cannot succeed with probability one. Therefore, it could be possible that maximally entangled states are sufficient to achieve perfect performance, whenever this can be done using some entangled state.

In a one-round two-party nonlocal game $G = (S, T, A, B, V, \pi)$, two isolated parties, commonly known as Alice and Bob, play against the verifier. The verifier chooses a pair of questions $(s, t) \in S \times T$ according to some probability distribution π and sends s to Alice and t to Bob. The players need to respond with $a \in A$ and $b \in B$ respectively. They win if $V(a, b|s, t) = 1$, where $V : A \times B \times S \times T \to \{0, 1\}$ is a public verification function. The players' goal is to coordinate strategies so as to maximize their probability of winning; quantum players can use shared entanglement to improve their chances of winning. We say that a strategy is *perfect* if it allows the players to win with probability one. Games which admit perfect finite-dimensional quantum but not classical strategies are known as *pseudo-telepathy* games [BBT05]. It is a challenging open question to understand if the optimal success probability of a game with finite question and answer sets can always be achieved using a finite-dimensional strategy. Hence, there might exist games with entangled value $\omega^*(G) = 1$ that are nevertheless not pseudo-telepathy according to our definition above (see [LTW13,Reg12,MV14] for examples in related settings). In this paper we avoid addressing the this above issue by dealing only with games which admit perfect finite-dimensional strategies. The central question of this paper is as follows:

Do there exist pseudo-telepathy games that cannot be won using maximally entangled state?

Answering the above question in the negative would imply that maximally entangled state is sufficient for zero-error communication over a noisy classical channel. This is due to the equivalence of zero-error communication protocols and a certain type of nonlocal games outlined in [CLMW10].

Previous results. It is known that maximally entangled state is sufficient for binary[1] and unique games[2] [CHTW04]. However, this is due to a trivial reason, since no entanglement is needed to win these games with probability one whenever it can be done using some entangled strategy. Therefore, these two classes of games do not contain any pseudo-telepathy games and hence are not relevant to our question. Maximally entangled state is also sufficient for the games based

---

[1] In a binary game Alice and Bob need to answer bits, *i.e.*, $S = T = \{0, 1\}$.

[2] In a unique game for every pair of questions $(s, t) \in S \times T$ there exists a permutation σ_{st}, such that $V(a, b|s, t) = 1$ if and only if $a = \sigma(b)$.

on graph homomorphisms [RM12] and binary constraint system games [CM12]. These two classes are more relevant, since they contain pseudo-telepathy games.

Our results. We partially answer the above question by exhibiting a class of games for which maximally entangled state is sufficient to reach perfect performance (see Theorem 1). The definition of this class is similar to that of projection games. This class subsumes both pseudo-telepathy graph homomorphism games and pseudo-telepathy binary constraint system games. In addition, we show that the answer to our central question is affirmative if and only if after the addition of consistency checks all pseudo-telepathy games remain pseudo-telepathy (see Theorem 3). Finally, our results show that any pseudo-telepathy weak projection game allows for a device independent certification of a maximally entangled state (see Corollary 2). As an application, we exhibit a family of games G_n that can be used to test for maximally entangled states of local dimension $\Omega(n)$ (see Corollary 3).

Our proof technique for Theorem 1 is inspired by the one used in [CMN+07] in the context of coloring games.

2   Preliminaries

Let $\mathrm{M}(d_A, d_B)$ denote the set of all complex $d_A \times d_B$ matrices. We use the mapping $\mathrm{vec} : \mathrm{M}(d_A, d_B) \to \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ defined via

$$\mathrm{vec} : |i\rangle\langle j| \mapsto |i\rangle|j\rangle$$

for all $i \in [d_A], j \in [d_B]$ and extended by linearity.

We now derive a formula that will often be used later. Applying the fact that $\mathrm{vec}(AXB^{\mathrm{T}}) = A \otimes B \, \mathrm{vec}(X)$ and $\mathrm{vec}(A)^\dagger \, \mathrm{vec}(B) = \mathrm{Tr}(A^\dagger B)$, and choosing matrix D such that $\mathrm{vec}\, D = |\psi\rangle$ we obtain

$$
\begin{aligned}
\mathrm{Tr}(A \otimes B|\psi\rangle\langle\psi|) &= \langle\psi|(A \otimes B)|\psi\rangle \\
&= \mathrm{vec}(D)^\dagger (A \otimes B) \, \mathrm{vec}(D) \\
&= \mathrm{vec}(D)^\dagger \, \mathrm{vec}(ADB^{\mathrm{T}}) \\
&= \mathrm{Tr}(D^\dagger ADB^{\mathrm{T}})
\end{aligned}
\tag{1}
$$

for all $A \in \mathrm{M}(d_A, d_A), B \in \mathrm{M}(d_B, d_B)$ and $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$.

Any bipartite state $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ with $d_A \leq d_B$ can be expressed as

$$|\psi\rangle = \sum_{i \in [d_A]} \lambda_i |\alpha_i\rangle|\beta_i\rangle \tag{2}$$

where $\lambda_i \geq 0$ and $\{|\alpha_i\rangle : i \in [d_A]\}$ is an orthonormal basis of $\mathbb{C}^{d_A}$ and the vectors $|\beta_i\rangle$ are orthonormal. This is known as a Schmidt decomposition of $|\psi\rangle$. (Note that the vec mapping shows that Schmidt decomposition is simply an alternative expression of the singular value decomposition.) The number of nonzero λ_i is

called the Schmidt rank of $|\psi\rangle$. We say that $|\psi\rangle$ has full Schmidt rank, if $d_A = d_B$ and $\lambda_i > 0$ for all i. We say that a state $|\psi\rangle$ is maximally entangled if all its Schmidt coefficients λ_i are the same.

Consider a state $|\psi\rangle \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ of full Schmidt rank. Then $d_A = d_B$ and $\mathrm{Tr}_A\,|\psi\rangle\langle\psi| = \mathrm{Tr}_B\,|\psi\rangle\langle\psi|$. Moreover, if we work in a Schmidt basis of $|\psi\rangle$, we have that

$$\mathrm{vec}\,\sqrt{\mathrm{Tr}_B(|\psi\rangle\langle\psi|)} = \mathrm{vec}\,\sqrt{\sum_i \lambda_i^2 |i\rangle\langle i|} = |\psi\rangle.$$

3   Technical lemmas

The goal of this section is to better understand the scenario where Alice and Bob each perform a measurement on some bipartite state $|\psi\rangle$ and obtain perfectly correlated outcomes. In the context of nonlocal games the following lemma states that maximally entangled state can be used in place of any shared entangled state whose reduced state on either party commutes with the corresponding party's measurement operators.

Lemma 1. *Let* $\{E_i\}_{i\in[n]}, \{F_i\}_{i\in[m]} \subseteq \mathrm{Pos}(\mathbb{C}^d \otimes \mathbb{C}^d)$ *be measurements. Also let* $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ *be a state of full Schmidt rank and* $D := \sqrt{\mathrm{Tr}_B\,|\psi\rangle\langle\psi|} = \sqrt{\mathrm{Tr}_A\,|\psi\rangle\langle\psi|}$.

If $[D, E_i] = 0$ *for all* $i \in [n]$ *or* $[D, F_i] = 0$ *for all* $i \in [m]$ *then for all* $i \in [n], j \in [m]$ *we have*

$$\mathrm{Tr}(E_i \otimes F_j |\psi\rangle\langle\psi|) = 0 \Leftrightarrow \mathrm{Tr}(E_i \otimes F_j |\Psi\rangle\langle\Psi|) = 0,$$

where $|\Psi\rangle := \frac{1}{\sqrt{d}} \sum_i |\alpha_i\rangle|\beta_i\rangle$ *and* $|\alpha_i\rangle|\beta_i\rangle$ *is a Schmidt basis of* $|\psi\rangle$.

Proof. Let us work in a Schmidt basis of $|\psi\rangle$. Then $\mathrm{vec}\,D = \mathrm{vec}\,\sqrt{\mathrm{Tr}_B\,|\psi\rangle\langle\psi|} = |\psi\rangle$. Since $\mathrm{Tr}(E_i \otimes F_j |\psi\rangle\langle\psi|) = \mathrm{Tr}(D^\dagger E_i D F_j^{\mathrm{T}})$ by Equation [(1)](#) and $D^\dagger E_i D, F_j^{\mathrm{T}} \succeq 0$, we obtain that

$$\mathrm{Tr}(E_i \otimes F_j |\psi\rangle\langle\psi|) = 0 \Leftrightarrow D^\dagger E_i D F_j = 0.$$

We now assume that $[D, E_i] = 0$ for all $i \in [n]$ (the other case can be proven similarly). Since $D^\dagger E_i D F_j^{\mathrm{T}} = D^\dagger D E_i F_j^{\mathrm{T}}$ and D has full rank, we have

$$D^\dagger E_i D F_j^{\mathrm{T}} = 0 \Leftrightarrow E_i F_j^{\mathrm{T}} = 0.$$

Observe that $\mathrm{vec}\,|\Psi\rangle = \mathrm{Id}$ and hence $\mathrm{Tr}(E_i \otimes F_j |\Psi\rangle\langle\Psi|) = \mathrm{Tr}(\mathrm{Id}^\dagger E_i\,\mathrm{Id}\,F_j^{\mathrm{T}}) = \mathrm{Tr}(E_i F_j^{\mathrm{T}})$. Thus we obtain

$$E_i F_j^{\mathrm{T}} = 0 \Leftrightarrow \mathrm{Tr}(E_i \otimes F_j |\Psi\rangle\langle\Psi|) = 0$$

which completes the proof. $\square$

In the context of local measurements, the following lemma states that only *projective* local measurements can give rise to perfectly correlated outcomes. Moreover, in such a case maximally entangled state $|\Psi\rangle$ can be used as the shared entangled state.

Lemma 2. *Let* $\{E_i\}_{i\in[n]}, \{F_i\}_{i\in[n]} \subseteq \mathrm{Pos}(\mathbb{C}^d \otimes \mathbb{C}^d)$ *be two measurements and* $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ *be a state of full Schmidt rank and* $D := \sqrt{\mathrm{Tr}_B |\psi\rangle\langle\psi|}$. *If for all distinct* $i, j \in [n]$

$$\mathrm{Tr}(E_i \otimes F_j |\psi\rangle\langle\psi|) = 0 \tag{3}$$

then for all $i \in [n]$ *we have that*

- *operators* E_i, F_i *are projectors and*
- $[D, E_i] = [D, F_i] = 0.$

Proof. First, note that D can be assumed to be diagonal, if we work in the Schmidt basis of $|\psi\rangle$ and hence $D^\dagger = D^\mathrm{T} = D$. Now we rewrite Equation (3) as

$$\mathrm{Tr}(D^\dagger E_i D F_j^\mathrm{T}) = 0, \tag{4}$$

for all distinct $i, j \in [n]$. It now follows that $\mathrm{Tr}\left(D^\dagger E_i D(\mathrm{Id} - F_i^\mathrm{T})\right) = 0$ and hence

$$\mathrm{supp}(D^\dagger E_i D) \subseteq \mathrm{supp}\, F_i^\mathrm{T},$$

where $\mathrm{supp}(M)$ denotes the span of the columns of M. Similarly, the fact that $\mathrm{Tr}\left((\mathrm{Id} - E_i)D F_i^\mathrm{T} D^\dagger\right) = 0$ gives

$$\mathrm{supp}(D F_i^\mathrm{T} D^\dagger) \subseteq \mathrm{supp}(E_i).$$

Since conjugation by full rank matrix D does not change the rank, the two above inclusions imply that

$$\mathrm{supp}\, F_i^\mathrm{T} = \mathrm{supp}(D^\dagger E_i D) \quad \text{and} \quad \mathrm{supp}(E_i) = \mathrm{supp}(D F_i^\mathrm{T} D^\dagger).$$

Combining this with the orthogonality constraints (4), we get that

$$\mathrm{supp}\, F_i^\mathrm{T} \perp \mathrm{supp}\, F_j^\mathrm{T} \ \text{and} \ \mathrm{supp}\, E_i \perp \mathrm{supp}\, E_j$$

for all distinct $i, j \in [n]$. Hence, both $\{E_i\}_{i\in[n]}$ and $\{F_i\}_{i\in[n]}$ are projective measurements and moreover

$$E_i = \mathrm{supp}(D F_i^\mathrm{T} D^\dagger) \text{ and } F_i^\mathrm{T} = \mathrm{supp}(D^\dagger E_i D),$$

where by slight abuse of notation we use $\mathrm{supp}(M)$ to denote the *projector* onto the span of the columns of M.

We now show that $[D, E_i] = 0$ for all $i \in [n]$ (the proof for $[D, F_i] = 0$ is similar). From the orthogonality condition (4) and the fact that $D^\dagger E_i D, F_j^\mathrm{T} \succeq 0$, we obtain that for all distinct $i, j \in [n]$

$$0 = D^\dagger E_i D F_j^\mathrm{T} = D^\dagger E_i D \, \mathrm{supp}(D^\dagger E_j D).$$

Hence, for all distinct $i, j \in [n]$ we also have $D^\dagger E_i D D^\dagger E_j D = 0$ and thus $E_i D^2 E_j = 0$, since D has full rank and $D^\dagger = D$. Now, $E_i D^2 E_j = 0$ implies that D^2 is block-diagonal with respect to the partition of the space corresponding to projectors E_i. Since in such a partition each E_i is block-diagonal with the blocks being $c\,\mathrm{Id}$, where $c \in \{0, 1\}$, it follows that $[D^2, E_i] = 0$. Hence also $[D, E_i] = 0$ for all $i \in [n]$ as desired. □

It follows from the proof of Lemma 2 that maximally entangled states are essentially the only states that give rise to perfectly correlated outcomes. Since the operators E_i and F_i commute with D, their off-diagonal entries corresponding to different Schmidt coefficients of $|\psi\rangle$ must be zero. Thus, the E_i and F_i are block-diagonal, where the blocks are labeled by distinct Schmidt coefficients of $|\psi\rangle$. Hence, the measurements $\{E_i\}$ and $\{F_i\}$ are direct sums of projective measurements each of which is performed on a maximally entangled state.

We now establish a result similar to Lemma 2 for two measurements with different number of outcomes.

Corollary 1. *Let* $\{E_i\}_{i \in [n]}, \{F_i\}_{i \in [m]} \subseteq \mathrm{Pos}(\mathbb{C}^d \otimes \mathbb{C}^d)$ *be two measurements and* $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ *be a state of full Schmidt rank and* $D := \sqrt{\mathrm{Tr}_B |\psi\rangle\langle\psi|}$. *If there exists a function* $f : [n] \to [m]$ *such that for all* $i \in [n]$ *and* $j \neq f(i)$

$$\mathrm{Tr}(E_i \otimes F_j |\psi\rangle\langle\psi|) = 0 \tag{5}$$

then for all $i \in [m]$ *we have that*

- *operators* $F_j, E'_j := \sum_{i:f(i)=j} E_i$ *are projectors and*
- $[D, E'_j] = [D, F_j] = 0$.

Proof. This is exactly the statement of Lemma 2 for measurements $\{E'_j\}_{j \in [m]}$ and $\{F_j\}_{j \in [m]}$. □

4   Weak projection games

We now define a class of nonlocal games for which we will later show that maximally entangled state can be used to win with certainty, whenever it can be done using some finite-dimensional quantum strategy.

Definition 1. *Let* $G = (S, T, A, B, V, \pi)$ *be a nonlocal game. We say that* G *is weakly projective for Bob, if for each of Bob's inputs* $t \in T$ *there exists an input* $s \in S$ *for Alice and a function* $f_{st} : A \to B$ *such that* $V(s, t, a, b) = 1$ *if and only if* $b = f_{st}(a)$.

The definition for a nonlocal game that is weakly projective for Alice is similar. We say that G *is a* weak projection *game if it is weakly projective for Bob or for Alice.*

The term "weak projection game" was chosen since G is called a projection game if for *all* pairs $(s,t) \in S \times T$ there exists a function f_{st} such that $V(s,t,a,b) = 1$ if and only if $f_{st}(a) = b$. Any projection game is weakly projective for both Alice and Bob; the converse, however, does not hold.

Theorem 1. *Suppose that a nonlocal game $G = (S,T,A,B,V,\pi)$ is weakly projective for Bob. If a shared entangled state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ of full Schmidt rank and measurements $\mathcal{E}^{(s)} := \{E_i^s\}_{i \in A}$ and $\mathcal{F}^{(t)} := \{F_i^t\}_{i \in B}$ specify a perfect strategy for G then*

1. *operators F_j^t are projectors for all $t \in T, j \in B$;*
2. *a maximally entangled state $|\Psi\rangle$ can be used in place of $|\psi\rangle$.*

Proof. To prove the theorem, for each $t \in T$ we apply Corollary 1 to measurements $\mathcal{E}^{(s(t))}$ and $\mathcal{F}^{(t)}$, where $s(t)$ is Alice's input corresponding to t from Definition 1. This gives us item (1) and that $[F_j^t, D] = 0$ for all values of t, j. Now, by Lemma 1 we get item (2). □

Recalling discussion after the proof of Lemma 2 we immediately obtain that weak projection games allow for self-testing of maximally entangled states.

Corollary 2. *Consider a pseudo-telepathy game $G = (S,T,A,B,V,\pi)$ which is weakly projective for Bob. Moreover, assume that any perfect strategy for G must use entanglement of local dimension at least d. Then any perfect strategy for G certifies the presence of a maximally entangled state of local dimension at least d.*

To illustrate how to apply the above corollary, let us consider coloring games of Hadamard graphs H_n [AHKS06]. The vertices of H_n are all the n-bit strings and two vertices are adjacent if the corresponding strings differ in exactly half of the positions. In the c-coloring game, Alice and Bob each get asked a vertex s and t respectively and they need to respond with the same color when $s = t$ and different colors when s is adjacent to t [CHTW04]. Let G_n be the game for n-coloring the Hadamard graph H_n. Like any of the coloring games, G_n is weakly projective. It is also known that G_n is a pseudo-telepathy game whenever $4|n$ and $n \geq 12$ [AHKS06,GN08].

Theorem 2. *Let $4|n$ and assume that $\mathcal{S}$ is a perfect strategy for G_n. Then S uses entanglement of local dimension at least $\Omega(n)$.*

The proof of Theorem 2 along with a detailed discussion can be found in Appendix A. The basic idea is to translate entangled strategies for G_n into one-way communication protocols for an appropriate communication version of G_n (a certain promise equality problem EQ_n). With this translation in hand, it only remains to obtain an appropriate lower on the one-way communication complexity of EQ_n, which we accomplish in Lemma 3. The general approach used to convert lower bounds in the communication setting to lower bounds on the dimension of the shared entanglement might be of independent interest.

Combining Theorem 2 with Corollary 2 immediately gives the following:

Corollary 3. *Let $n \in \mathbb{N}$ be such that $4|n$ and $n \geq 12$. Any perfect strategy for the coloring game G_n certifies the presence of a maximally entangled state of dimension at least $\Omega(n)$.*

5   Games with added consistency checks

Given a nonlocal game G, we now define a new game by adding consistency check questions for one of the parties.

Definition 2. *Given game $G = (S, T, A, B, V, \pi)$, let $\tilde{G}_B := (S, T, \tilde{A}, B, \tilde{V}, \pi)$, where*

$$\tilde{S} := \{(s, 0), (t, 1) : s \in S, t \in T\},$$

$\tilde{A} := A \cup B$, *and*

$$\tilde{V}(a, b|(s, i), t) := \begin{cases} V(a, b|s, t) & \text{if } i = 0 \\ \delta_{ab} & \text{if } i = 1 \end{cases}$$

The game $\tilde{G}_A$ is defined similarly.

It is easy to see that $\tilde{G}_A$ ($\tilde{G}_B$) is a weak projection game for Alice (Bob) and therefore can be won using a maximally entangled state whenever some perfect quantum strategy exists. Also, any strategy used to win $\tilde{G}_A$ or $\tilde{G}_B$, can be used to win G. Hence, we obtain the following:

Theorem 3. *A nonlocal game G admits a perfect finite-dimensional quantum strategy if and only if $\tilde{G}_A$ or $\tilde{G}_B$ admits some perfect finite-dimensional quantum strategy.*

The above theorem can be used to show that a maximally entangled state is sufficient for both binary constraint system and homomorphism games.

In a binary constraint system game G, Alice is asked to assign values to the binary variables in a constraint c_s and Bob is asked to assign a value to a binary variable x_t. To win, their answers need to be consistent and Alice's assignment has to satisfy the constraint c_s. Any strategy used to win game G can also be used to win $\tilde{G}_B$. This is because upon receiving input $(t, 1)$ Alice can perform any measurement corresponding to a constraint c_s that contains variable x_t and respond with the value she would have assigned to the variable x_t.

In a homomorphism game G, Alice and Bob have the same input and output sets ($S = T$ and $A = B$) and their answers need to agree when they are given the same outputs. Therefore, any strategy used to win G can be used to win both $\tilde{G}_A$ and $\tilde{G}_B$ (essentially by ignoring the extra bit in the modified game).

6   Discussion

In this paper we have looked at the question of whether there exist pseudo-telepathy games that cannot be won with certainty using a maximally entangled

state in some dimension d. As partial progress towards answering this question we have exhibited a class of pseudo-telepathy games for which maximally entangled state is always sufficient. Additionally, we have characterized pseudo-telepathy games which admit perfect strategies with a maximally entangled state. We hope that this characterization might help in producing an example of pseudo-telepathy which does not admit a maximally entangled perfect strategy (assuming such games exist).

An intersting open question is whether Lemma 2 admits an approximate version. More formally: suppose two measurements produce almost perfectly correlated outcomes, does it imply that the measurement operators almost commute with the reduced state D?

References

ADGL02.   Antonio Acín, Thomas Durt, Nicolas Gisin, and José I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65(5):052325, 2002. arXiv:quant-ph/0111143.

AGG05.   Antonio Acín, Richard Gill, and Nicolas Gisin. Optimal Bell tests do not require maximally entangled states. *Phys. Rev. Lett.*, 95(21):210402, 2005. arXiv:quant-ph/0506225.

AHKS06.   David Avis, Jun Hasegawa, Yosuke Kikuchi, and Yuuya Sasaki. A quantum protocol to win the graph colouring game on all Hadamard graphs. *IEICE Trans. Fundamentals*, 89(5):1378–1381, 2006. arXiv:quant-ph/0509047.

BBL$^+$15. Jop Briët, Harry Buhrman, Debbie Leung, Teresa Piovesan, and Florian Speelman. Round elimination in exact communication complexity. In *Proceedings of TQC'15*, 2015.

BBT05.   Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005. arXiv:quant-ph/0407221.

BCW98.   Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of STOC'98*, pages 63–68, 1998. arXiv:quant-ph/9802040.

BRSDW11. Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald De Wolf. Near-optimal and explicit Bell inequality violations. In *Proceedings of CCC'11*, pages 157–166, 2011. arXiv:1012.5043.

CHTW04.   Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of CCC 2004*, pages 236–249, 2004. arXiv:quant-ph/0404076.

CLMW10.   Toby S. Cubitt, Debbie Leung, William Matthews, and Andreas Winter. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.*, 104:230503–230506, 2010. arXiv:0911.5300.

CM12.   Richard Cleve and Rajat Mittal. Characterization of binary constraint
            system games, 2012. arXiv:1209.2729.
CMN⁺07.   Peter J. Cameron, Ashley Montanaro, Michael W. Newman, Simone Sev-
            erini, and Andreas Winter. On the quantum chromatic number of a graph.
            Electr. J. Comb., 14(1), 2007. arXiv:quant-ph/0608016.
dW01.   Ronald de Wolf. *Quantum Computing and Communication Complexity.*
            PhD thesis, Universiteit van Amsterdam, 2001.
FR87.   Peter Frankl and Vojtěch Rödl. Forbidden intersections. *Trans. Amer.
            Math. Soc.*, 300(1):259–286, 1987. doi:10.2307/2000598.
GN08.   Chris D. Godsil and Michael W. Newman. Coloring an or-
            thogonality graph. *SIAM J. Discrete Math.*, 22(2):683–692, 2008.
            arXiv:math/0509151.
Gru99.   Jozef Gruska. *Quantum Computing.* Osborne/McGraw-Hill, 1999.
JP11.   Marius Junge and Carlos Palazuelos. Large violation of Bell inequalities
            with low entanglement. *Commun. Math. Phys.*, 306(3):695–746, 2011.
            arXiv:1007.3043.
Lov79.   László Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inf.
            Theory*, 25(1):1–7, Jan 1979. doi:10.1109/TIT.1979.1055985.
LTW13.   Debbie Leung, Ben Toner, and John Watrous. Coherent state exchange in
            multi-prover quantum interactive proof systems. *Chic, J. Theor. Comput.*,
            2013(11), 2013. arXiv:0804.4118.
LVB11.   Yeong-Cherng Liang, Tamás Vértesi, and Nicolas Brunner. Semi-device-
            independent bounds on entanglement. *Phys. Rev. A*, 83(2):022108, 2011.
            arXiv:1012.1513.
MV14.   Laura Mančinska and Thomas Vidick. Unbounded entanglement can
            be needed to achieve the optimal success probability. In *Proceedings of
            ICALP'14*, volume 8572 of *LNCS*, pages 835–846, 2014. arXiv:1402.4145.
NC10.   Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quan-
            tum information.* Cambridge university press, 2010.
PV07.   Martin B. Plenio and Shashank Virmani. An introduction to entanglement
            measures. *Quant. Inf. Comput.*, 7:1–51, 2007. arXiv:quant-ph/0504163.
Reg12.   Oded Regev. Bell violations through independent bases games. *Quantum
            Inf. Comput.*, 12(1-2):9–20, 2012. arXiv:1101.0576.
RM12.   David E. Roberson and Laura Mančinska. Graph homomorphisms for
            quantum players. 2012. arXiv:1212.1724.
VW11.   Thomas Vidick and Stephanie Wehner. More nonlocality with less entan-
            glement. *Phys. Rev. A*, 83:052310, May 2011. arXiv:1011.5206.
Yao79.   Andrew C.-C. Yao. Some complexity questions related to distributive
            computing (preliminary report). In *Proceedings of STOC'79*, pages 209–
            213, 1979. doi:10.1145/800135.804414.
ZG08.   Stefan Zohren and Richard D. Gill. Maximal violation of the Collins-Gisin-
            Linden-Massar-Popescu inequality for infinite dimensional states. *Phys.
            Rev. Lett.*, 100(12):120406, 2008. arXiv:quant-ph/0612020.

A   Communication protocols from entangled strategies

Communication complexity was first introduced by Yao [Yao79] and there have been several examples where results in the communication setting have been translated to nonlocal games. Here notable examples include Hidden Matching problem [BRSDW11] and coloring of Hadamard graphs, which can be seen as a certain promise equality problem [BCW98]. In both cases separations between the quantum and classical communication complexity were translated into separations between the entangled and classical values of the game.

In the communication setting the goal of two separated parties, Alice and Bob, is to compute a joint function $f(s,t)$, where input $s \in S$ is given to Alice and $t \in T$ to Bob. We focus on one-way communication protocols, where, after receiving her input s, Alice sends a message m_s to Bob who must then correctly output $f(s,t)$. The communication cost of such a protocol is the length of the message m_s (measured in bits or qubits) for the worst case input s. Consequently, the communication complexity of f is the minimum communication cost over all valid protocols. Let us stress that throughout this section we only consider the setting where Bob must always announce the correct value of $f(s,t)$.

We are interested in the deterministic one-way communication complexity, $D^1(f)$, and its quantum analogue $Q_0^1(f)$ and in our case f is a certain promise equality problem EQ_n (*i.e.*, partial function). For this problem, the input sets S and T are the vertices of the Hadamard graph H_n where $4|n$, *i.e.*, n-bit binary strings. The promise is that either $s = t$ or s is adjacent to t (strings s and t differ in exactly half of the positions) and Bob must announce which case it is. In other words, $EQ_n(s,t) := \delta_{st}$ for the allowed input pairs (s,t). In general, if $EQ(X)$ is the equality problem with the promise that the parties are either given equal or adjacent vertices of a graph X, then $D^1(EQ_n) = \log(\chi(X))$, where $\chi(X)$ is the chromatic number of X [dW01]. It now follows that $D^1(EQ_n) = \log(\chi(H_n)) = \Omega(n)$ since the chromatic number of Hadamard graphs H_n is exponential in n for $n = 4m$ [FR87,AHKS06]. To determine the quantum communication complexity $Q_0^1(EQ_n)$, it is useful to consider a relaxation of coloring, called orthogonal representation. In such a representation, for each vertex $s \in V(X)$ we want to assign a unit vector $|v_s\rangle \in \mathbb{C}^d$ so that adjacent vertices receive orthogonal vectors. The orthogonal rank of X, denoted $\xi(X)$, is the smallest dimension d in which X admits an orthogonal representation. Similar to the classical case, it is known that $\log(\xi(X)) = Q_0^1(EQ(X))$ [BBL$^+$15].

Lemma 3. *Let $4|n$. Then $Q_0^1(EQ_n) = \log\big(\xi(H_n)\big) = \log n$.*

Proof. When Lovàsz introduced his Theta function in [Lov79], he showed that Theta of the complement, $\vartheta(\overline{X})$, lower bounds the orthogonal rank $\xi(X)$ for any graph X. Combining this with the fact that $\vartheta(\overline{H_n}) = n$ [RM12], we obtain that $\xi(H_n) \geq n$. To see that $\xi(H_n) \leq n$, it suffices to note that

$$|v_s\rangle = \frac{1}{\sqrt{n}} \sum_{i \in [n]} (-1)^{s_i} |i\rangle \tag{6}$$

gives an n-dimensional orthogonal representation of H_n. To conclude the proof we use the fact that $Q_0^1(\mathrm{EQ}_n) = \xi(H_n)$. □

We summarize the one-way communication complexities for promise equality problems in Table 1.

	EQ(X)	$EQ(H_n) = EQ_n$
One-way deterministic c.c., D^1	$\log\left(\chi(X)\right)$	$\Omega(n)$
One-way exact quantum c.c., Q_0^1	$\log\left(\xi(X)\right)$	$\log n$

Table 1. One-way communication complexity of promise equality problems

According to Lemma 3, any exact one-way quantum communication protocol for EQ_n must use messages of length $\log n$. We would like to transfer this lower bound to the nonlocal games setting (recall the definition of the games G_n from page 7). To this end, we consider a simple construction for converting entangled strategies for G_n to one-way communication protocols for EQ_n. In fact, a similar construction can be used to relate strategies for any coloring game on a graph X to one-way communication protocols for the promise equality problem $\mathrm{EQ}(X)$.

Communication protocol for EQ_n from an entangled strategy for G_n. Consider a perfect entangled strategy $\mathcal{S}$ for the nonlocal game G_n. Let $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be the shared entangled state used in $\mathcal{S}$. Also let $\mathcal{A}^s$ and $\mathcal{B}^t$ be the measurements they apply upon receiving s and t respectively. In the communication setting, upon receiving input s, Alice prepares the bipartite state $|\psi\rangle$ and measures its first register using $\mathcal{A}^s$. She then sends the measurement outcome $a \in [n]$ along with the second register of the state to Bob. This requires communication of $\log n$ classical bits and $\log d$ qubits. After receiving the quantum state, Bob measures it using $\mathcal{B}^t$ and compares the outcome of his measurement, b, to Alice's outcome a that she had sent over. He announces that $s = t$, if $a = b$ and otherwise he says that $s \neq t$. The correctness of Bob's answer follows directly from the fact that the strategy $\mathcal{S}$ is perfect for G_n.

We now show that quantum one-way communication protocols for EQ_n in which Alice also sends Bob a small amount of classical information do not allow for significant savings in the quantum communication cost. In combination with the above translation of entangled strategies into communication protocols this will allow us to lower bound the dimension of the entanglement needed for a perfect strategy of G_n.

Lemma 4. *Let $\mathcal{P}$ be an exact one-way communication protocol for the promise equality problem EQ_n which uses $\log n$ classical bits and $\log d$ qubits. Then $d = \Omega(n)$, i.e., the quantum communication cost of $\mathcal{P}$ is $\Omega(\log n)$.*

Proof. Without loss of generality, we can assume that Alice's actions in the protocol $\mathcal{P}$ are deterministic. That is, upon receiving input $s \in \{0,1\}^n$ she transmits a classical message m_s of at most $\log n$ bits and a quantum state

$|\psi_s\rangle \in \mathbb{C}^d$. The messages m_s give rise to a partition of the vertex set of the Hadamard graph H_n into induced subgraphs $\{L_m : m \in \{0,1\}^{\log n} \cong [n]\}$. Therefore, $\mathcal{P}$ can be used to obtain one-way quantum communication protocols of cost $\log d$ for each of the promise equality problems $\mathrm{EQ}(L_m)$. Therefore,

$$\log\big(\xi(L_m)\big) = Q_0^1\big(\mathrm{EQ}(L_m)\big) \leq \log d. \tag{7}$$

Since $\chi(X) \leq (1 + 2\sqrt{2})^{2\xi(X)}$ for any graph X [CMN$^+$07], we obtain that

$$\chi(L_m) \leq (1 + 2\sqrt{2})^{2d} < 14^d. \tag{8}$$

Therefore, $D\big(\mathrm{EQ}(L_m)\big) \leq \log(14^d) < 3d$ for all $m \in [n]$. Together with the classical messages m_s from the protocol $\mathcal{P}$ this yields a deterministic one-way communication protocol for EQ_n of cost $\log n + 3d$. By Lemma 3, we get that $\log n + 3d = \Omega(n)$ and hence $d = \Omega(n)$ as desired. $\qquad\square$

We are now ready to establish a lower bound on the amount of entanglement required in any perfect strategy for n-coloring the Hadamard graph H_n.

Theorem 2. *Let $4|n$ and assume that $\mathcal{S}$ is a perfect strategy for G_n. Then S uses entanglement of local dimension at least $\Omega(n)$.*

Proof. Consider any perfect strategy $\mathcal{S}$ for G_n and let d be the local dimension of the shared entangled state employed in $\mathcal{S}$. The above construction (see page 12) allows us to convert $\mathcal{S}$ into an exact one-way communication protocol for EQ_n which uses $\log n$ bits and $\log d$ qubits. By Lemma 4 we get that $d = \Omega(n)$ as desired. $\qquad\square$